

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:

APPLE IPHONE, IMEI (FROM SIM TRAY):
357274096819800;

Magistrate No. 20-129 MJ

LG PHONE, IDENTIFIER: ZNFL713DL; ITEM: 1B27

Magistrate No. 20-130 MJ

SAMSUNG GALAXY S4, IMEI: 357738055036754

Magistrate No. 20-131 MJ

FBI POSSESSION ON SITE OF SEARCH

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

INTRODUCTION AND AGENT BACKGROUND

I, James A. Simpson, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and say:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B .

2. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code.

3. I have been employed with the Federal Bureau of Investigations (“FBI”) for the past twelve (12) years. I began my career in March 2008, when I underwent basic law

enforcement training at the FBI Academy in Quantico, Virginia. Upon graduation from the Academy, I was initially assigned to the FBI Newark Field Office, where I worked Hispanic drug trafficking and computer intrusions until December 2014. I was then transferred to my current assignment at the FBI Laurel Highlands Resident Agency Pittsburgh Field Office. In my current position, among other duties, I oversee the Southwest Pennsylvania Safe Streets Task Force ("SWPSSTF") and have been so assigned since December 2014. The SWPSSTF is an intergovernmental law enforcement task force comprised of federal, state, and local enforcement officers who are specially deputized to serve as federal Task Force Officers ("TFO") authorized to participate in and conduct investigations into violations of federal law. The SWPSSTF's investigative focus consists of, but is not limited to, violations of the federal Controlled Substances Act, 21 U.S.C. § 801, et seq., violent crime, and criminal gang activity.

4. In my capacity as a Special Agent with the FBI, I have been involved in more than one hundred federal and/or state investigations and have personally arrested or directly assisted in the arrests of drug law violators. I have participated in numerous investigations involving the unlawful distribution and possession with the intent to distribute controlled substances, including cocaine, heroin, fentanyl, crack cocaine, and methamphetamine, in violation of Title 21, United States Code, Sections 841 and 846. These investigations have utilized a variety of investigative techniques such as undercover officers, informants, confidential sources, sources of information, physical surveillance, electronic surveillance, pen registers, telephone toll analysis, and search warrants. I have personally served as the affiant on search warrants in drug investigations which have discovered evidence and led to the successful prosecution of the targets. Through my involvement in these narcotics investigations, I have handled cooperating sources of information who were involved in narcotics acquisition and/or

trafficking. Additionally, I have reviewed thousands of communications between drug traffickers through review of cell phones seized pursuant to drug investigations. I have had hundreds of conversations with drug traffickers, drug users, and other members of law enforcement regarding the methods and language used by drug traffickers to smuggle, store, and distribute drugs and to collect and launder drug distribution proceeds.

5. Further, based on my training and experience, I am aware that it is common practice for drug traffickers who desire to insulate themselves from detection by law enforcement to routinely utilize multiple telephones, counter surveillance, false or fictitious identities, and coded communications in order to communicate with their customers, suppliers, couriers, and co-conspirators. Moreover, it is not unusual for drug traffickers to initiate or subscribe such phone services in fictitious names or under the name of an associate or family member in an effort to thwart detection by law enforcement. Also, it is now a common practice for drug traffickers to utilize all communication features of their telephones, most notably the voice call and text message features, nearly simultaneously, to communicate with their conspirators and customers. For example, it is quite common for a particular transaction to be set up and completed using both voice calls and text messages. In fact, it is now quite unusual for a drug trafficker to utilize solely one feature of a telephone, such as the voice call feature, to further his criminal activities while not also using another feature, such as the text message feature, to further his criminal activities.

6. Additionally, I have participated as the co-affiant, case agent, and monitor in a Title III wiretap investigation. Through this experience, as well as by way of additional training, I am familiar with the technical aspects of wiretap investigations, including the call monitoring process, transcription of pertinent calls, minimization requirements, and physical surveillance

component. Through this experience, I am familiar with the coded language employed by drug traffickers to disguise the substance of their oral and textual communications.

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

RELEVANT CRIMINAL STATUTES

8. Under Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(C), it is unlawful for any person to knowingly, intentionally and unlawfully possess with intent to distribute and distribute a quantity of a mixture and substance containing a detectable amount of heroin, a Schedule I controlled substance, and/or fentanyl, a Schedule II controlled substance, and/or crack cocaine, a Schedule II controlled substance, and/or cocaine, a Schedule II controlled substance.

9. Under Title 21, United States Code, Section 846, it is unlawful for any two or more persons to knowingly, intentionally and unlawfully conspire with one another to possess with intent to distribute and distribute a quantity of a mixture and substance containing a detectable amount of heroin, a Schedule I controlled substance, and/or fentanyl, a Schedule II controlled substance, and/or crack cocaine, a Schedule II controlled substance, and/or cocaine, a Schedule II controlled substance, contrary to the provisions of Title 21, United States Code, Sections 841(a)(1) and 841(b)(1)(C).

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

10. The property to be searched is:

- 1) Apple Iphone IMEI (From SIM Tray): 357274096819800;
- 2) LG Phone Identifier: ZNFL713DL; Item: 1B27;
- 3) Samsung Galaxy S4 IMEI: 357738055036754;

hereinafter the "Devices." The Devices are currently in the possession of the FBI.

11. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

12. The Devices, as previously stated, are currently in the lawful possession of the FBI. As will be described in further detail below, they came into the FBI's possession during a Court of Common Pleas search warrant executed at 102 Gap Avenue, Johnstown, Pennsylvania (PA).

13. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

FACTS AND CIRCUMSTANCES

14. In September of 2019, the SWPSSTF received information from a confidential informant (CI1)¹ and other investigative means that Curel LIVINGSTON was selling heroin and/or fentanyl, cocaine, crack cocaine, and prescription drugs in and around Johnstown, PA. Investigators learned through their investigation that LIVINGSTON would promote himself to his customers as a poly-drug distributor and would send out multimedia messages containing his "menu" of drug types, and the quantities and prices he offered each for sale, complete with weekly specials and bulk-buy discounts.² Law enforcement subsequently conducted three

¹ Information provided by CI1 has proven reliable in the past and has been corroborated through controlled buys and other investigative means by law enforcement.

² Investigators possess a copy of the multimedia message "menu" LIVINGSTON sent to CI1. During a search of LIVINGSTON's residence, TFOs also found a dry-erase board drug "menu", as well, which listed types, quantities, and prices of various controlled substances.

controlled drug buys³ for various controlled substances that LIVINGSTON and/or his girlfriend Marie ENGELBRECHT were purported to be selling. Also through the course of the investigation, through surveillance, TFOs identified where the Defendant and his then girlfriend, resided during the months leading up to the lawful search warrant executed in November 2019 at LIVINGSTON's residence located at 102 Gap Avenue, Johnstown, PA.

15. During the first controlled drug buy on September 17, 2019 and the second controlled buy on October 15, 2019, CI1 contacted LIVINGSTON at phone number (814) 691-3641, which he/she advised LIVINGSTON had provided as his phone number. Law enforcement successfully purchased controlled substances from LIVINGSTON on both instances⁴ arranged via contact over LIVINGSTON's phone ((814) 691-3641).

16. On November 14, 2019, following a third controlled drug buy at 102 Gap Avenue⁵, a lawful search warrant was obtained and executed at the aforementioned location.

3 A "controlled buy" is a purchase of a controlled substance by a CI/Undercover Officer ("UC") under the direct control and supervision of a police investigator. If a CI is utilized, the CI is searched for drugs and currency prior to the purchase. His/her vehicle (if it is to be utilized) is also searched for drugs and currency prior to the transaction. The CI/UC is followed to and from the point of purchase and visual contact is attempted to be maintained at all times, except when he/she has actually entered any structure where the purchase is to take place. After the purchase, the CI/UC is followed back to a predetermined location where the drugs are relinquished to the investigating officer(s) and the CI, and any vehicle utilized by the CI, is again searched. When practicable and lawful, the CI/UC is equipped with recording equipment to attempt to capture an audio/video recording of the deal. Law enforcement followed these procedures during each of the controlled purchases described herein.

4 During the first controlled buy, investigators purchased alprazolam from LIVINGSTON. During the second, officers bought crack cocaine.

5 Investigators arranged this third controlled buy for marijuana. The marijuana involved in this controlled buy was left on the porch of 101 Gap Avenue by Marie ENGELBRECHT for the CI to pick up. The CI was directed to leave the money for the marijuana on the porch. Surveillance officers watched ENGELBRECHT stash the quantity of marijuana to be sold on the porch, observed the CI approach, take the marijuana and leave the money, and then witnessed ENGELBRECHT step back out onto the porch and recover the money left by the CI.

Upon entering the residence on the morning of the search, TFOs provided LIVINGSTON with his Miranda warnings. LIVINGSTON then volunteered that he wanted to cooperate with investigators. He told officers that they would find some “work” (crack cocaine) in a safe along with a .45 caliber pistol. He also told officers that he possessed a shotgun, as well, but that he was holding both firearms for a friend. LIVINGSTON also directed officers where to find the key for the safe(s).

17. Officers located the keys and two safes, one (“Safe X”) in one bedroom (“Bedroom X”), and the second (“Safe Z”) in another bedroom (“Bedroom Z”). Inside Safe Z, officers found a gallon-sized Ziploc bag of marijuana. Also in Bedroom Z, TFOs discovered a false-bottom Bluetooth speaker containing numerous vials of suspected crack cocaine. In Safe X, among other items, TFOs found an additional, large quantity of crack cocaine, \$3,570 cash, a .45 caliber pistol, a loaded magazine, additional .45 caliber rounds, and .12 gauge shotgun shells. Between these two safes and other hiding spots within the residence, TFOs recovered a total of 179.65 grams of crack cocaine, 3.46 grams of heroin/fentanyl, 1.495 grams of heroin, 21.81 grams of cocaine, and 239.41 grams (just over a half-pound) of marijuana. They also recovered drug trafficking paraphernalia (digital scales, a money counter, owe sheets, a dry-erase board drug menu) and indicia for LIVINGSTON (driver’s license, checks).

18. In addition, law enforcement seized several phones during the search of 102 Gap Avenue. Investigators recovered an **Apple iPhone IMEI (From SIM Tray): 357274096819800** (hereinafter, “**Apple iPhone**”) and **LG Phone Identifier: ZNFL713DL; Item: 1B27** (hereinafter “**LG Phone**”) from Bedroom Z, where they also found narcotics and other contraband related to drug trafficking. Officers also found a **Samsung Galaxy S4 IMEI: 357738055036754** in a bathroom closet. LIVINGSTON identified the **Apple iPhone** and the

LG Phone as his phones and provided the passcodes for each. Law enforcement confirmed that phone number (814) 691-3641, which the CI had contacted to arrange the controlled buys on September 17, 2019 and October 15, 2019, belonged to the **Apple iPhone**.

19. In combination, the facts described above provide probable cause that the aforementioned “devices” which were seized at 102 Gap Avenue have been used to arrange and conduct and/or facilitate narcotics transactions, and that evidence of these violations of 21 U.S.C. §§ 841, 843, and 846 will be found within the information requested herein. Your affiant respectfully submits that the facts give rise to the issuance of a search warrant for these aforementioned electronic devices.

EVIDENCE COMMONLY STORED ON CELL PHONES AND OTHER ELECTRONIC STORAGE DEVICES

20. Based on my training and experience, I am aware that it is a common practice for drug traffickers who desire to insulate themselves from detection by law enforcement to routinely utilize multiple telephones, counter surveillance, false or fictitious identities, and coded communications to communicate with their customers, suppliers, couriers, and other conspirators. It is not unusual for drug traffickers to initiate or subscribe such phone or phone device services under the names of other real or fictitious people. Moreover, it is now a very common practice for drug traffickers to utilize all communication features of their telephones, most notably the voice call and text message features, nearly simultaneously to communicate with their co-conspirators.

21. I am aware that evidence of drug, firearm, and money laundering crimes can often be found in electronic media, including cellular telephones, laptop computers, cameras, and tablet devices. Such evidence can be found throughout those items, such as in text messages,

contact lists indicating the names and numbers of associates, call/text logs indicating calls/texts made to and received from associates, online search history files, word processing documents, and photograph and video gallery files. Additionally, with the advancement of cellular phones, specifically “smart phones”, one can use their cell phone as a GPS. Locations and addresses can be contained on one’s cellular phone. It should be noted that, with the advance of technology, the distinction between computers and cellular telephones has become less clear. Actions such as internet searching or emailing, in addition to calling and text messaging and photographing, can now be performed from many cell phones. In addition, as noted above, those involved in drug trafficking crimes commonly communicate using multiple cellular telephones.

Contemporaneous possession of multiple cellular telephones is, therefore, evidence of such trafficking. Moreover, the particular numbers of, and the particular numbers dialed by, particular cellular telephones can be evidence of drug trafficking, particularly in light of the fact that it is a practical necessity that drug traffickers communicate with each other, as well as with their customers and suppliers, by telephone. Such numbers can confirm identities of particular associates and the occurrence of certain events.

22. As with most electronic/digital technology items, communications made from an electronic device, such as a cellular telephone or a standard computer, are often saved or stored on the device. Storing this information can be intentional, for example, by saving a text message or a contact or an e-mail. Digital information can also be retained unintentionally. Traces of the path of an electronic communication, an internet search, and the locations of photographs and videos may be automatically stored in many places on a computer or cellular telephone. In addition to electronic communications, a user’s internet activities generally leave traces in the web cache and internet history files. A forensic examiner often can recover evidence that shows

when and in what manner a user of an electronic device, such as a computer or a cell phone, used such a device.

23. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they often can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on an electronic storage device such as a computer, the data contained in the file often does not actually disappear; rather, that data often remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on a device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from an electronic storage device depends less on when the file was sent, downloaded, or viewed than on a particular user's operating system, storage capacity, and habits.

24. I am aware that those who illegally possess drugs sometimes take trophy photographs and videos using their cameras and/or cellular telephones of their drugs, firearms, and proceeds and retain them on those devices. In addition, I am aware that drug traffickers, like law-abiding citizens, sometimes take photographs and videos using their cameras and cellular

telephones of themselves with their friends, relatives, and associates and keep the photographs and videos on those devices. When they are taken or retained by drug traffickers, such photographs and videos can be evidence, and can lead to additional evidence, of illegal trafficking activity by identifying the traffickers, contraband, and people who are actively assisting and/or supporting the trafficking activity as well as the locations where they live or where they store their drugs, firearms, proceeds, or paraphernalia.

25. It should be noted that data on electronic communication and/or storage devices is often relevant to a criminal investigation by revealing who used a particular device. In addition, such data can reveal who resided at or who had access to a particular location if, for example, a particular device was found at a particular location (e.g., inside a particular room of a particular residence) and the device contains data demonstrating that it was used by or belonged to a particular person. In that sense, a particular electronic device can be significant indicia linking a particular person to contraband or other criminal activity even if the device itself does not contain the remnants of incriminating communications.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

26. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

Forensic Evidence: Deleted Files, User Attribution

27. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this

forensic electronic evidence might be on the Device because data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

29. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

30. Records, communications stored at the time the warrant is served (i.e., no real-time communications will be intercepted and searched during service), data, and textual and graphic files (including photographs and videos), evidencing who used the device and/or when and/or from where, or evidencing violations of Title 21, United States Code, Sections 841 and/or 846.

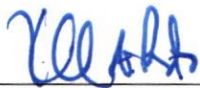
CONCLUSION

31. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B and I request that the Court issue the proposed search warrant.

The above information is true and correct to the best of my knowledge, information and belief.

/s/ James A. Simpson
JAMES A. SIMPSON
Special Agent, FBI

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 20 day of July, 2020.



KEITH A. PESTO
United States Magistrate Judge